INSO

8232-9

1st. Edition

2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران

۸۲۳۲-۹

چاپ اول

۱۳۹۲

کارت‌های شناسایی- کارت‌های مدارمجتمع- قسمت۹: دستورهایی برای مدیریت کارت

Identification cards - Integrated circuit cards - Part 9: Commands for card management

ICS:35.240.15

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« کارت‌های شناسایی– کارت های مدارمجتمع– قسمت۹: دستور هایی برای مدیریت کارت»

رئیس:	**سمت و/ یا نمایندگی**
محسن‌زاده، علی اکبر (فوق لیسانس مخابرات)	کارشناس تدوین پیش‌نویس استانداردهای ملی
دبیر:	
روشن‌بخش، علی (لیسانس اقتصاد)	کارشناس مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
افکار، علی (دکتری الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت
تورانی، فرزام (لیسانس مهندسی کامپیوتر)	کارشناس فنی مرکز تحقیقات صنایع انفورماتیک
حنیفه، فرشته (لیسانس اقتصاد)	کارشناس مرکز تحقیقات صنایع انفورماتیک
زندباف، عباس (لیسانس مهندسی الکترونیک-مخابرات)	کارشناس شرکت ارتباطات زیرساخت
نادری، مجید (دکترای مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد "کارت‌های شناسایی– کارت‌های مدارمجتمع– قسمت۹: دستورهایی برای مدیریت کارت" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات صنایع انفورماتیک، به‌عنوان استاندارد ملی ایران، تهیه شده و در صد و هفتاد و پنجمین اجلاسیه‌ی کمیته‌ی ملی استاندارد خدمات مورخ ۹۲/۹/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

منبع و مأخذی که برای تهیهٔ این استاندارد به‌کار گرفته شده، به شرح زیر است:

ISO/IEC 7816-9: 2004, Identification cards _ Integrated circuit cards _ Part 9: Commands for card management

« کارت‌های شناسایی– کارت‌های مدارمجتمع– قسمت۹: دستورهایی برای مدیریت کارت»

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین دستورهای بین صنعت برای مدیریت کارت و پرونده است. این دستورها تمام چرخه عمر کارت را پوشش می‌دهند و لذا بعضی از دستورها را ممکن است پیش از اینکه کارت برای دارنده آن صادر شود یا پس از انقضای کارت استفاده کرد.

این استاندارد، پیاده‌سازی داخلی درون کارت و/یا خارج آن را پوشش نمی‌دهد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 7816-4: Identification cards- Integrated circuit cards – Part 4: Organization, security and commands for interchange

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاح و تعریف زیر به‌کار می‌رود:

۱-۳

پیام رسانی ایمن

مجموعه‌ای از ابزار برای حفاظت رمز شده از (یا قسمتی از) زوج‌های دستور- پاسخ [ISO/IEC 7816-4]

۴ کوته نوشت‌ها

کوته‌نوشت‌ها و سرواژه‌های زیر در این استاندارد به‌کار می‌روند:

۱-۴	**APDU** [1]	واحد داده های پروتکل کاربرد
۲-۴	**FCP** [2]	متغیرهای کنترل پرونده
۳-۴	**LCS** [3]	وضعیت چرخه عمر

1 - Application protocol data unit
2 - File control parameters
3 - Life cycle status

۵ چرخه عمر

وضعیت چرخه عمر ممکن است مربوط به هر شیءی پیوسته به کارت یا مربوط به خود کارت باشد. کارت مورد نظر، از وضعیت چرخه عمر در ترکیب با خصوصیات امن دیگر، به‌منظور تعیین اینکه آیا یک عملیات بر روی یک شیء بر طبق یک خط‌مشی امن است، استفاده خواهد کرد. وضعیت چرخه عمر بازتابی از به‌کارگیری شیءها بر طبق مقررات زیر است:

- اگر یک شیء در مرحله ایجاد است، هیچ خصیصه امن برای آن شیء اعمال نخواهد شد.
- اگر یک شیء در مرحله آغازین است، ممکن است هر خصیصه امن خاص این مرحله را اعمال کرد.
- اگر یک شیء در مرحله عملیات است، هر خصیصه امن مرتبط اعمال خواهد شد.
- اگر یک شیء در مرحله پایانی است، ارزش شیء تغییر نخواهد یافت بلکه ممکن است از شیءآن‌طورکه مشخصه‌های امن مرتبط مشخص کرده‌اند استفاده کرد، برای مثال ممکن است آن را حذف کرد.

گذر بین وضعیت‌های اولیه چرخه عمر، برگشت ناپذیر است و فقط از زمان ایجاد تا پایان رخ می‌دهد. به علاوه، کاربرد ممکن است وضعیت‌های چرخه عمر ثانویه‌ای را تعیین کند؛ هر وضعیت اولیه ممکن است وضعیت‌های چرخه عمر ثانویه برگشت‌پذیری را تعیین کند. تغییرات توسط کارت کنترل می‌شوند و ممکن است به ترتیبی از پیش تعریف شده انجام شوند که تغییرات برگشت‌پذیر یا برگشت‌ناپذیر در وضعیت‌ها را انعکاس می‌دهند. دستورهای زیر برای مدیریت کارت و پرونده را ممکن است برای راه‌اندازی یک وضعیت گذر چرخه عمر به‌کار برد.

EF را خاتمه بده [۱]

پرونده را فعال کن [۲]

پرونده ایجاد کن [۳]

DF را خاتمه بده [۴]

پرونده را غیر فعال کن [۵]

پرونده را حذف کن [۶]

استفاده از کارت را خاتمه بده [۷]

زمانی که دستورها اجرا می‌شوند ممکن است ارزش وضعیت چرخه عمر را تعیین کنند. در هر حال، کارت باید تمامیت این ارزش را در انطباق با این استاندارد حفظ کند.

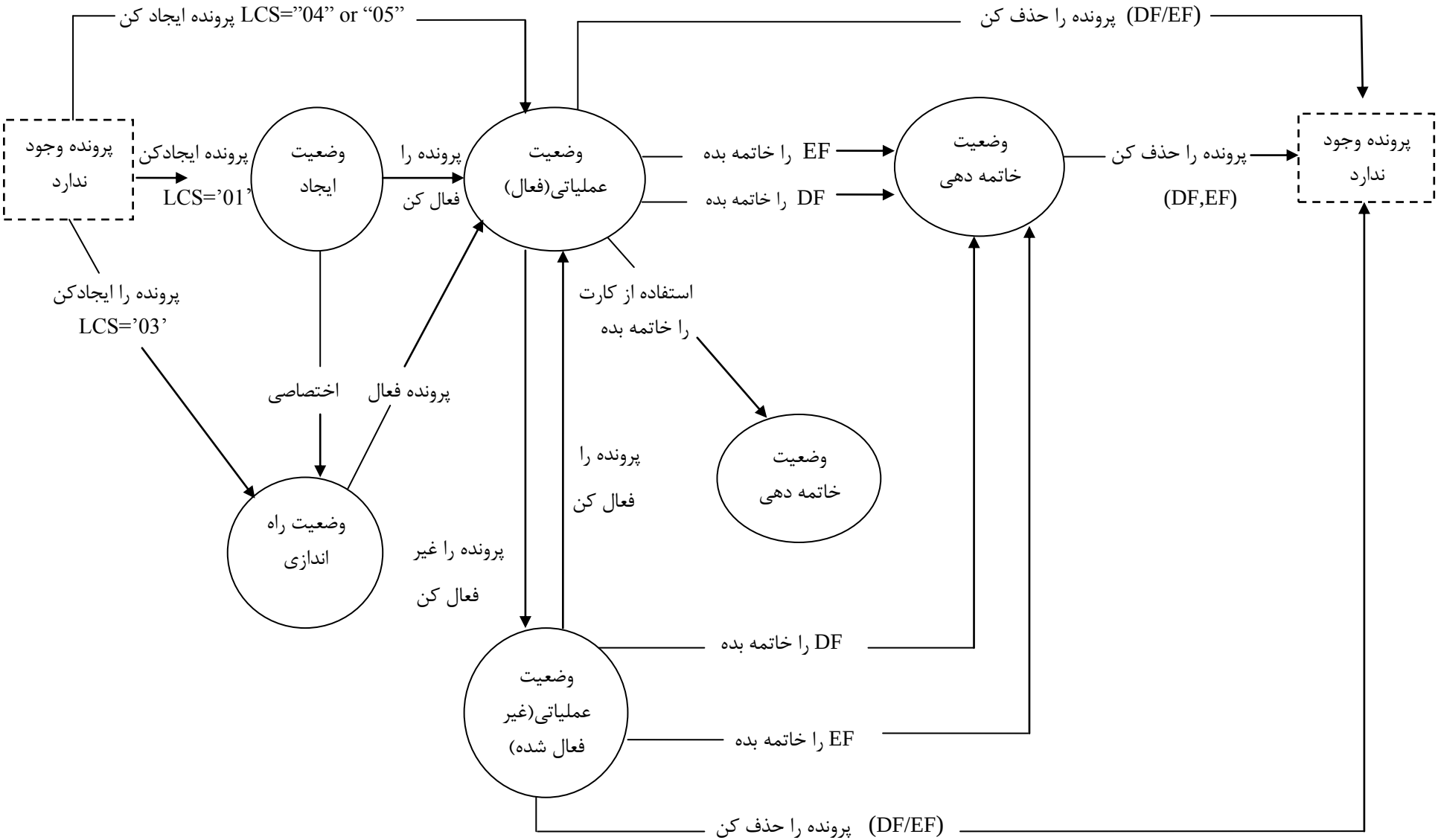
---

1 - TERMINATE EF
2 - ACTIVATE FILE
3 - CREATE FILE
4 - TERMINATE DF
5 - DEACTIVATE FILE
6 - DELETE FILE
7 - TERMINATE CART USAGE

۵-۱ چرخه عمر فایل [۱]

شکل ۱ نمایشی ذهنی از وضعیت‌های چرخه عمر پرونده و دستوری است که موجب یک گذر، پس از اتمام موفقیت‌آمیز می‌شود. این شکل شرایط اجرای آن دستورها را نشان نمی‌دهد. (استاندارد ISO/IEC 7816-4 مراجعه شود)

[۱] پرونده



شکل ۱- نمودار چرخه عمر پرونده

۶ دستورهایی برای مدیریت کارت

برای تمام کارت‌هایی که از این استاندارد برای پشتیبانی دستورها و گزینه هایی که فرمان را پشتیبانی می کنند یا تمام گزینه های فرمانی نباید اجباری شود.

دستورها را فقط در صورتی می‌توان اجرا کرد که وضعیت امن، مشخصه‌های امن دستور را برآورده کنند.

بیت‌های ۳ و ۴ برای این دستورها بی معنی هستند و بهتر است نادیده گرفته شوند.

برای هر دستور فهرست ناقصی از شرایط وضعیت ارائه شده است. (استاندارد ISO/IEC 7816-4 را هم ببینید.)

۶-۱ دستور ایجاد پرونده (CREATE FILE COMMAND)

دستور پرونده ایجاد کن (CREATE FILE)، ایجاد یک پرونده (DF یا EF) را راه می‌اندازد که بلافاصله در زیر DF جاری قرار می‌گیرد. این دستور مجاز است تا به پرونده‌ای که ایجاد می‌کند، حافظه تخصیص دهد. پرونده ایجاد شده به‌عنوان پرونده جاری قرار خواهد گرفت مگر اینکه به‌گونه‌ای دیگر تعیین شده باشد.

رفتار کارت در موردی که در DF، واحدی بیش از یک EF دارای یک شناسه EF کوتاه مفروض، وجود داشته باشد، در این استاندارد تعریف نشده است.

این دستور را فقط در صورتی می‌توان اجرا کرد که وضعیت امن، مشخصه‌های امن دستور را بر آورده کند.

بایت توصیف‌گر پرونده، اجباری است و نشان می‌دهد که آیا قرار است یک DF یا یک EF ایجاد شود.

- اگر یک DF ایجاد شده است، بهتر است یک نام DF و/یا یک شناسه پرونده تعیین شود.
- اگر یک EF ایجاد شده است، بهتر است یک شناسه پرونده و/یا یک شناسه کوتاه EF مشخص شود.

جدول ۱- زوج پاسخ - دستور پرونده ایجاد کن (CREATE FILE)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است
INS	‘E0’
P1-p2	شناسه پرونده ’0000‘ و متغیرهای پرونده که در فیلد داده‌های دستور کد شده‌اند. P1 که برابر ’00‘ نیست: بایت توصیف‌گر پرونده است. P2 شناسه کوتاه EF بر روی بیت‌های ۸ تا ۴ است؛ بیت‌های ۳ تا ۱ اختصاصی هستند.
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدان Data	شابلون FCP (برچسب ۶۲) و شابلون‌های احتمالی دیگر یا غایب
میدان Le	در صورت کد کردن Ne=0 ، غایب است.

میدان Data	وجود ندارد.
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول‌های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982، 6A84، 6A89 و 6A8A

یادآوری- اگر شماره Nc صفر باشد، در آن صورت پرونده ایجاد شده دارای متغیرهای کنترل پرونده پیش فرض (Default) خواهد بود.

۶-۲ دستور حذف پرونده (DELETE FILE)

دستور پرونده را حذف کن (DELETE FILE)، حذف یک EF مورد اشاره که بلافاصله زیر DF جاری قرار دارد یا یک DF با تمام زیر شاخه‌هایش را آغاز می‌کند. پس از پایان موفقیت‌آمیز این دستور، پرونده حذف شده را دیگر نمی‌توان انتخاب کرد. پرونده جاری پس از حذف یک EF ، DF جاری است. DF جاری پس از حذف یک DF ، DF مادر است، مشروط بر اینکه به‌گونه‌ای دیگر تعیین نشده باشد. منابعی که توسط پرونده نگه‌داشته شده بوده است آزاد خواهند شد و حافظه‌ای را که این پرونده استفاده می‌کرده به وضعیت پاک‌شده منطقی درخواهد آمد.

حذف پرونده ممکن است علاوه بر آن به وضعیت عمر پرونده وابسته باشد. MF حذف نخواهد شد.

اگر ’0000‘ =P1-P2 باشد و میدان Dataی دستور وجود نداشته باشد، در این صورت دستور به پرونده‌ای اعمال خواهد شد که توسط دستوری انتخاب شده باشد که درست قبل از این اجرا شده است. علاوه بر این، چنانچه پرونده انتخابی بر روی کانال منطقی دیگری انتخاب شده باشد، اجرای دستور لغو می‌شود و در پاسخ، کد خطای مربوطه برگردانده خواهد شد.

سایر معانی P1-P2 و از جمله مقرراتی که منحصر به‌فرد بودن شناسه‌ها را تعریف می‌کند، در دستور انتخاب کن (SELECT) تشریح شده‌اند.

جدول ۲- زوج پاسخ - دستور پرونده را حذف کن(DELETE FILE)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.
INS	‘E4’
P1-P2	’0000‘ پرونده جاری را حذف می‌کند. سایر مقادیر آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدان Data	آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Le	در صورت کد کردن Ne=0 ، غایب است.

میدان Data	وجود ندارد.
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول‌های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982 و 6985

۶-۳ دستور غیرفعال کردن پرونده (DEACTIVATE FILE)

دستور پرونده را غیرفعال کن (DEACTIVATE FILE)، غیرفعال کردن قابل برگشت یک پرونده را آغاز می‌کند. پس از پایان موفقیت‌آمیز این دستور، علاوه بر دستور انتخاب کن (SELECT)، فقط دستورهای

پرونده را فعال کن (ACTIVATE FILE)، پرونده را حذف کن (DELETE FILE)، دستور ختم EF (TERMINATE EF) و در مورد یک DF دستور ختم DF (TERMINATE DF) مجاز خواهند بود.
زمانی که نسبت به یک پرونده غیرفعال شده به‌کار می‌رود، دستور انتخاب کن (SELECT) پرونده را انتخاب و SW1-SW2 =’6283’ را به‌عنوان یک وضعیت هشدار با مضمون: پرونده انتخابی اعتبار ندارد یعنی غیرفعال است، بر می‌گرداند.
اگر یک EF انتخاب شده باشد، در این صورت دستور فقط نسبت به EF و نه به DF مادر، اعمال خواهد شد.
اگر P1-P2= ‘0000’ باشد و میدان Dataی دستور وجود نداشته باشد، در این صورت دستور به پرونده‌ای اعمال خواهد شد که توسط دستوری انتخاب شده باشدکه درست قبل از این اجرا شده است. سایر معانی P1-P2 و از جمله مقرراتی که منحصر به‌فرد بودن شناسه‌ها را تعریف می‌کند، در دستور انتخاب کن (SELECT) تشریح شده‌اند.
توصیه می‌شود از پیغام‌رسانی ایمن استفاده شود. چنانچه واحد داده‌های پروتکل کاربرد (APDU) پاسخ‌دهی، حفاظت نشده باشد، در این صورت شیوه بررسی اینکه کار به‌درستی اجرا شده است، در دامنه کاربرد استاندارد ISO/IEC 7816 قرار ندارد.
به‌دلایل امن، به‌دست آوردن همین عملکرد از طریق ابزار اختصاصی، مجاز است.

جدول ۳- زوج پاسخ- دستور پرونده را غیرفعال کن (DEACTIVATE FILE)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.
INS	‘04’
P1-P2	‘0000’ پرونده جاری را غیرفعال می‌کند. سایر مقادیر آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدانData	آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Le	در صورت کد کردن Ne=0 غایب است.

میدان Data	وجود ندارد.
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982 و 6A80

۴-۶ دستور فعال کردن پرونده (ACTIVATE FILE)

دستور پرونده را فعال کن (ACTIVATE FILE)، تغییر وضعیت یک پرونده را از وضعیت ایجاد یا وضعیت آغازین یا وضعیت عملیاتی غیرفعال شده به وضعیت عملیاتی فعال شده، راه‌اندازی می‌کند.

فعال کردن پرونده‌ای که به‌طور صحیح ایجاد شده باشد همواره مجاز است. فعال کردن یک پرونده غیرفعال شده تنها در صورتی می‌تواند انجام شود که وضعیت امن، مشخصه‌های امن تعریف شده برای این پرونده به‌منظور عملیات فعال‌سازی را برآورده کند.

چنانچه واحد داده‌های پروتکل کاربرد (APDU) پاسخ‌دهی، به‌وسیله پیغام‌رسانی ایمن حفاظت نشده باشد، در این صورت شیوه بررسی اینکه کار به‌درستی اجرا شده است، در دامنه کاربرد استاندارد ISO/IEC 7816 درج نشده است.

اگر ’0000‘ =P1-P2 باشد و میدان Dataی دستور وجود نداشته باشد، در این صورت دستور به پرونده‌ای اعمال خواهد شد که توسط دستوری انتخاب شده باشدکه درست قبل از این اجرا شده است. سایر معانی P1-P2 و از جمله مقرراتی که منحصر بفرد بودن شناسه‌ها را تعریف می‌کند، در دستور انتخاب کن (SELECT) تشریح شده‌اند.

جدول۴- زوج پاسخ - دستور پرونده را فعال کن (ACTIVATE FILE)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.
INS	’44‘
P1-P2	’0000‘ پرونده جاری را فعال می‌کند. سایر مقادیر آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود)
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدان Data	آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Le	در صورت کد کردن Ne=0 غایب است.

میدان Data	وجود ندارد
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول‌های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6400 و 6982

۶-۵ دستور ختم DF (TERMINATE DF)

دستور DF را خاتمه بده (TERMINATE DF) گذر غیرقابل بازگشت یک DF را به وضعیت پایانی راه‌اندازی می‌کند.

پس از یک پایان موفقیت‌آمیز این دستور، DF در یک وضعیت پایانی است و از قابلیت کارکردی موجود DF و زیر شاخه‌هایش کاسته شده است. DF قابل انتخاب خواهد بود و در صورت انتخاب شدن، موقعیت هشدار SW1-SW2 =’6285’ (به معنی پرونده انتخابی در وضعیت پایانی است) برگردانده خواهد شد. در استاندارد ISO/IEC 7816 ، سایر اعمال ممکن درج نشده است.

یادآوری- غرض از خاتمه دادن به DF معمولاً این است که کاربرد کارت را برای دارنده کارت، غیر قابل استفاده کنند.

به‌دلایل امن، به‌دست آوردن همین عملکرد از طریق ابزار اختصاصی، مجاز است.
اگر ’0000‘ =P1-P2 باشد و میدان Dataی دستور وجود نداشته باشد، در این صورت دستور به پرونده‌ای اعمال خواهد شد که توسط دستوری انتخاب شده باشدکه درست قبل از این اجرا شده است. سایر معانی P1-P2 و از جمله مقرراتی که منحصر به‌فرد بودن شناسه‌ها را تعریف می‌کند، در دستور انتخاب کن (SELECT) تشریح شده‌اند.
توصیه می‌شود از پیغام‌رسانی ایمن استفاده شود. چنانچه واحد داده‌های پروتکل کاربرد (APDU) پاسخ‌دهی، بوسیله پیغام‌رسانی ایمن حفاظت نشده باشد، در این صورت شیوه بررسی اینکه کار به‌درستی اجرا شده است، در دامنه کاربرد استاندارد ISO/IEC 7816 تشریح نشده است.

جدول۵- زوج پاسخ- دستور DF را خاتمه بده (TERMINATE DF)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.
INS	’E6‘
P1-P2	’0000‘ ، DF جاری را خاتمه می‌دهد. سایر مقادیر آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدان Data	آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Le	در صورت کد کردن Ne=0 غایب است.

میدان Data	وجود ندارد.
SW1-SW2	استاندارد ISO/IEC 7816-4، جدول‌های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982 و 6985

یادآوری- در دستورهایی که P1 P2 بر طبق دستور SELECT کد شده‌اند، (استاندارد ISO/IEC 7816-4 مراجعه شود.) بیت‌های ۳ و ۴ در P2 هیچ معنایی نداشته و بهتر است نادیده گرفته شوند.

۶-۶ دستور ختم EF (TERMINATE EF)

دستور EF را خاتمه بده (TERMINATE DF) گذر غیرقابل بازگشت EF تعیین شده را به وضعیت پایانی راه‌اندازی می‌کند.
EFی که قرار است خاتمه یابد، باید در یک وضعیت فعال‌شده یا غیرفعال شده باشد.
به‌دلایل امن، به‌دست آوردن همین عملکرد از طریق ابزار اختصاصی، مجاز است.
اگر ’0000‘ =P1-P2 باشد و میدان Dataی دستور وجود نداشته باشد، در این صورت دستور به پرونده‌ای اعمال خواهد شد که توسط دستوری انتخاب شده باشدکه درست قبل از این اجرا شده است. سایر معانی

P1-P2 و از جمله مقرراتی که منحصر به‌فرد بودن شناسه‌ها را تعریف می‌کند، در دستور انتخاب کن (SELECT) تشریح شده‌اند.

جدول۶- زوج پاسخ- دستور EF را خاتمه بده (TERMINATE EF)

CLA	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است.
INS	‘E8’
P1-P2	’0000‘ ، EF جاری را خاتمه می‌دهد. سایر مقادیر آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Lc	در صورت کد کردن Nc=0 غایب است ولی برای کد Nc>0 وجود دارد.
میدان Data	آن‌طور است که برای دستور SELECT تعریف شده است. (استاندارد ISO/IEC 7816-4 مراجعه شود.)
میدان Le	در صورت کد کردن Ne=0 غایب است.

میدان Data	وجود ندارد
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982 و 6985

۶-۷ دستور ختم استفاده از کارت (TERMINATE CART USAGE)

دستور استفاده از کارت را خاتمه بده (TERMINATE CART USAGE)، گذر غیرقابل بازگشت کارت را به وضعیت پایانی راه‌اندازی می‌کند.

در مورد کارت‌هایی که این دستور را پشتیبانی می‌کنند توصیه می‌شود که وضعیت پایانی، در گزینه پاسخ به بازنشانی (Answer-to-Reset) بیان شود.

پس از پایان موفقیت‌آمیز این دستور، کارت دستور SELECT را پشتیبانی نخواهد کرد.

به‌دلایل امن، به‌دست آوردن همین عملکرد از طریق ابزار اختصاصی، مجاز است.

یادآوری- هدف از خاتمه دادن به استفاده از کارت این است که کارت را برای دارنده کارت، غیر قابل استفاده کنند.

توصیه می‌شود از پیغام‌رسانی ایمن استفاده شود. چنانچه واحد داده‌های پروتکل کاربرد (APDU) پاسخ‌دهی، به‌وسیله پیغام‌رسانی ایمن حفاظت نشده باشد، در این صورت شیوه بررسی اینکه کار به‌درستی اجرا شده است، در دامنه کاربرد استاندارد ISO/IEC 7816 تشریح نشده است.

جدول۷- زوج پاسخ- دستور استفاده از کارت را خاتمه بده (TERMINATE CART USAGE)

CLA INS P1-P2	آن‌طور که در استاندارد ISO/IEC 7816-4 تعریف شده است. ‘FE’ ‘0000’
میدان Lc	در صورت کد کردن Nc=0 غایب است.
میدان Data	وجود ندارد.
میدان Le	در صورت کد کردن Ne=0 غایب است.

میدان Data	وجود ندارد.
SW1-SW2	استاندارد ISO/IEC 7816-4 ، جدول های ۵ و ۶ در مواردی که مرتبط است مراجعه شود، برای مثال 6982 و 6985

پیوست الف

(اطلاعاتی)

مثال هایی از خصیصه‌های امن که برای بارکردن به‌کار می‌روند

الف-۱ مقدمه

این مثال نشان می‌دهد که چگونه بار گذاری داده‌ها به داخل کارت (بارکردن امن) را از طریق درست‌سنجی حق دستیابی به هستار بار شونده و حفاظت از داده‌های ارسالی از طریق پیغام‌رسانی ایمن، کنترل کنیم. داده‌های بار شده مجازند که برای مثال شامل کُد، کلیدها و برنامه‌های کاربردی کوچک باشند.

فرض بر این است که:

- سامانه پرونده بر اساس این استاندارد است؛
- ساختار دستور، چرخه عمر و کنترل دستیابی بر اساس این استاندارد است؛
- DF جاری از قبل در وضعیت عملیاتی بوده است (LCS=۴)؛
- داده‌ها به داخل یک پرونده شفاف کمکی ۱ بار شود (DF/EF در وضعیت آغازین هستند (LCS=۳))؛
- در DF جاری، برای LCS=۳ داریم SEID= ۲ ، وضعیت آغازین است و ارتباطات برخط (online) است؛
- در DF جاری، برای LCS=۳ داریم SEID= ۳ ، وضعیت آغازین است و ارتباطات برون‌خطی (offline) است؛
- در DF جاری، برای LCS=۴ داریم SEID= ۴ و وضعیت عملیاتی است؛
- داده‌ها به‌منظور اعتباربخشی، به‌وسیله شیءهای داده‌ای پیغام‌رسانی ایمن، حفاظت (و در صورت تمایل رمزی) می‌شوند؛
- در یک ارتباطات برخط (SEID= ۲)، یک فرایند اعتباربخشی غیرمتقارن مثلاً با استفاده از تبادل کلید نشست قبلاً اجرا شده است، تا از طریق پیغام‌رسانی ایمن، از بارکردن حفاظت شود؛ داده‌هایی که قرار است بار شوند، توسط یک شیء داده‌ای مجموع مقابله‌ای رمز نگاری و در صورت تمایل توسط یک شیء داده‌ای رمزی، حفاظت می‌شوند؛
- در یک ارتباطات برون‌خطی (SEID= ۳)، داده‌هایی که قرار است بار شوند، توسط یک شیءداده‌ای امضای دیجیتال و در صورت تمایل توسط یک شیءداده‌ای رمزنگاری، رمزی و حفاظت می‌شوند؛
- اطلاعات مجوز (اجازه قانونی دارنده گواهینامه) ممکن است در یک جواز قابل تصدیق توسط کارت که هستار بارشونده را به کلید مجوز(SEID=۲، ارتباطات برخط) یا به کلید امضای دیجیتال (SEID= ۳، ارتباطات برون‌خطی) پیوند می‌دهد، وجود داشته باشد.

الف-۲ بارگیری ایمن

بارگیری ایمن تحت ارتباطات برخط و برون‌خطی، در زیر توضیح داده شده است.

ارتباطات برخط

۱. DF جاری را انتخاب کنید. (SELECT(DFنام=AID))
۲. برای ارتباطات برخط، وضعیت آغازین را قرار دهید. (MSE: RESTORE SEID= ۲)
۳. اعتباربخشی بیرونی (گواهینامه را درست‌سنجی کنید، اعتباربخشی بیرونی کنید.)
۴. پرونده ۱ را انتخاب کنید. ((شناسه پرونده)SELECT)
۵. داده‌ها را به درون پرونده بار کنید. (مثلاً WRITE BINARY) با SM، حفاظت‌شده توسط شیء داده‌ای مجموع مقابله‌ای رمزنگاری
۶. فعال کردن پرونده (ACTIVATE FILE)
۷. وضعیت عملیاتی را برقرار کنید. (MSE: RESTORE SEID= ۴)
۸. اعتبار کاربر را درست‌سنجی کنید. ((گذر واژه) VERIFY)
۹. پرونده ۱ را انتخاب کنید. ((شناسه پرونده) SELECT)
۱۰. اطلاعات را بخوانید. (READ BINARY)

ارتباطات برون‌خطی

۱. DF جاری را انتخاب کنید. (SELECT(DFنام=AID))
۲. برای ارتباطات برون‌خطی، وضعیت آغازین را قرار دهید. (MSE: RESTORE SEID= ۳)
۳. درست‌سنجی گواهینامه (VERIFY CERTIFICATE)
۴. پرونده ۱ را انتخاب کنید. ((شناسه پرونده)SELECT)
۵. داده‌ها را به درون پرونده بار کنید. (مثلاً WRITE BINARY) با SM حفاظت‌شده توسط شیءداده‌ای امضای دیجیتال
٦. فعال کردن پرونده (ACTIVATE FILE)
۷. وضعیت عملیاتی را برقرار کنید. (MSE: RESTORE SEID= ۴)
۸. اعتبار کاربر را درست‌سنجی کنید. ((گذر واژه) VERIFY)
۹. پرونده ۱ را انتخاب کنید. ((شناسه پرونده) SELECT)
۱۰. اطلاعات را بخوانید. (READ BINARY)

الف-۳ کُد کردن در قالب فشرده برای خصیصه‌های امنیت

کُدهای زیر نشان می‌دهند که دسترسی در وضعیت عملیاتی ممکن است از دسترسی در وضعیت آغازین متفاوت باشد.

ارتباطات بر خط

چنانچه برای یک وضعیت امن معین، در وضعیت آغازین اجازه یک دستور WRITE BINARY و (پس از اتمام موفقیت‌آمیز آن) یک دستور ACTIVATE FILE داده شده باشد و در وضعیت عملیاتی اجازه یک دستور READ BINARY داده شده باشد، در این صورت کُد بایت AM و بایت‌های SC به‌صورت زیر هستند.

- وضعیت آغازین
  - بایت AM ((1= بیت۳) WRITE BINARY)، (1= بیت۵) ACTIVATE FILE)
  - بایت۱ SC ((1= بیت۷) پیغام‌رسانی ایمن برای دستور ACTIVATE FILE)، (1= بیت۸) تمام شرایط)
  - بایت۲ SC ((11= بیت‌های ۷ تا ۶) اعتباربخشی بیرونی و پیغام‌رسانی ایمن برای WRITE BINARY)، (1= بیت۸) تمام شرایط)
- وضعیت عملیاتی
  - بایت AM ((1= بیت۱) READ BINARY)
  - بایت SC ((1= بیت۵) اصالت‌سنجی)

یکی از این دو:

- در بایت‌های SC، بیت‌های ۴ تا ۱ را یک شناسه SE کُد کنید (۲ به‌صورت 0010 و ۴ به‌صورت 0100)
- یا اینکه SE مرتبط به‌عنوان SE جاری (0000) شناخته می‌شود که در این صورت مشخصه‌های امن، در قالب گسترده کُد می‌شوند.

ارتباطات برون‌خطی

چنانچه برای یک وضعیت امن معین، در وضعیت آغازین اجازه یک دستور WRITE BINARY و (پس از اتمام موفقیت‌آمیز آن) یک دستور فعال داده شده باشد و در وضعیت عملیاتی اجازه یک دستور READ BINARY داده شده باشد، در این صورت کُد بایت AM و بایت‌های SC به‌صورت زیر هستند.

- وضعیت آغازین
  - بایت AM ((1= بیت۳) WRITE BINARY)، (1= بیت۵) فعال)
  - بایت۱ SC ((1= بیت۷) پیغام‌رسانی ایمن برای دستور ACTIVATE FILE)، (1= بیت۸) تمام شرایط)
  - بایت۲ SC ((1= بیت۷) اعتباربخشی بیرونی و پیغام‌رسانی ایمن برای WRITE BINARY)، (1= بیت۸) تمام شرایط)
- وضعیت عملیاتی
  - بایت AM ((1= بیت۱) READ BINARY)
  - بایت SC ((1= بیت۵) اصالت‌سنجی)

یکی از این دو:

- در بایت‌های SC، بیت‌های ۱تا۴ را یک شناسه SE کُد کنید. (۳ به‌صورت 0011 و ۴ به‌صورت 0100)
- یا اینکه SE مرتبط به‌عنوان SE جاری (0000) شناخته می‌شود که در این صورت مشخصه‌های امنیت، در قالب گسترده کُد می‌شوند.

الف-۴ کُد کردن در قالب گسترده برای خصیصه‌های امنیت

ارتباطات بر خط

چنانچه برای یک وضعیت امن معین، در وضعیت آغازین اجازه یک دستور WRITE BINARY و (پس از اتمام موفقیت‌آمیز آن) یک دستور ACTIVATE FILE داده شده باشد و در وضعیت عملیاتی اجازه یک دستور READ BINARY داده شده باشد، در این صورت کُد کردن شیءهای داده‌های AM و شیءهای داده‌های SC، احتمالاً به‌صورت زیر هستند.

- وضعیت آغازین
  - شیء داده‌های AM شماره ۱، یک بایت AM را منتقل می‌کند ((1= بیت۳)WRITE BINARY)
  - شیء داده‌های SC شماره ۱، یک AT شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های توصیف‌کننده کاربرد CRT را برای اعتباربخشی بیرونی (1= بیت۸)، منتقل می‌کند.
  - شیء داده‌های SC شماره ۲، یک CCT شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های کاربرد CRT را برای پیغام‌رسانی ایمن (11= بیت‌های ۵ تا ۶)، منتقل می‌کند.
  - شیء داده‌های AM شماره ۲، یک بایت AM را منتقل می‌کند ((1= بیت۵)ACTIVATE FILE)
  - شیء داده‌های SC شماره ۳، یک CCT شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های کاربرد CRT را برای پیغام‌رسانی ایمن (11= بیت‌های ۵ تا ۶) ، منتقل می‌کند.
- وضعیت عملیاتی
  - شیء داده‌های AM، یک بایت AM را منتقل می‌کند ((1= بیت۱) READ BINARY).
  - شیء داده‌های SC، یک AT شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های توصیف‌کننده کاربرد CRT که نشان‌دهنده اعتباربخشی کاربر(1= بیت۴) است را منتقل می‌کند.

SE مرتبط، به‌عنوان SE جاری (0000 = بیت‌های ۱ تا ۴) شناخته می‌شود که در این صورت مشخصه‌های امنیت، در قالب گسترده کُد می‌شوند.

ارتباطات برون خطی

چنانچه برای یک وضعیت امن معین، در وضعیت آغازین اجازه یک دستور WRITE BINARY و (پس از اتمام موفقیت‌آمیز آن) یک دستور ACTIVATE FILE داده شده باشد و در وضعیت عملیاتی اجازه یک دستور READ BINARY داده شده باشد، در این صورت کُد کردن شیءهای داده‌های AM و شیءهای داده‌های SC، به‌صورت زیر هستند.

- وضعیت آغازین
  - شیء داده‌های AM شماره ۱، یک بایت AM ((1= بیت ۳)WRITE BINARY)، ((1= بیت۵)ACTIVATE FILE) را منتقل می‌کند
  - شیء داده‌های SC شماره ۱، یک DST شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های توصیف‌کننده کاربرد CRT را برای پیغام‌رسانی ایمن (11= بیت‌های ۵ تا ۶) ، منتقل می‌کند.
- وضعیت عملیاتی
  - شیء داده‌های AM، یک بایت AM ((1= بیت۱) READ BINARY) را منتقل می‌کند.
  - شیء داده‌های SC، یک AT شامل یک شیء داده‌های ارجاع اصلی و یک شیء داده‌های توصیف‌کننده کاربرد CRT که نشان‌دهنده اعتباربخشی کاربر (1= بیت۴) است را منتقل می‌کند.

SE مرتبط، به‌عنوان SE جاری شناخته می‌شود که در این صورت مشخصه‌های امنیت، در قالب گسترده کُد می شوند.

الف-۵ کُد کردن محیط‌های امن متناظر

- SEID= ۲ در داخل شابلون (‘7B’)
- {‘95’ – {ارجاع اصلی { ‘80’ – L – ‘02’} – { ‘8A’ – L – ‘03’} – { ‘A4’ – L – {‘83’ – L - {‘5F4B’ – L – {80 – 01 مجوز دارنده گواهینامه - L – ‘83’} – {‘B4’ – L – {{ ارجاع اصلی { {‘30’ – ‘01’ – ‘95’} –
-
- SEID= ۳ در داخل شابلون (‘7B’)
- {‘95’ – {ارجاع اصلی { ‘80’ – L – ‘03’} – { ‘8A’ – L – ‘03’} – {‘B6’ – L – {‘83’ – L - {‘30’ – ‘01’}}
- SEID= ۴ در داخل شابلون (‘7B’)
- {‘95’ – {ارجاع اصلی { ‘80’ – L – ‘04’} – { ‘8C’ – L – ‘04’} – {‘A4’ – L – {‘83’ – L - {‘08’ – ‘01’}}